UNITED STATES DISTRICT COURT
SOUTH DISTRICT OF FLORIDA

MARY JANE WHALEN and CHRISTINE V. RONA, individually and on behalf of all others similarly situated, Plaintiffs, v. **GUNSTER, YOAKLEY & STEWARD, PA** Defendant.	Case No. 9:24-CV-80612 **SECOND AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Mary Jane Whalen, as Trustee of the Non-GST Exempt Management Trust f/b/o Mary Jane Whalen u/a/d 4/16/1993, ("Trustee" and the "Trust"), and Mary Jane Whalen ("Whalen"), personally and individually (together, "Whalen") and Christine V. Rona ("Rona" and, together with Whalen, "Plaintiffs"), on behalf of all others similarly situated, bring this action against Gunster, Yoakley & Steward, PA ("Gunster"). The following allegations are based on Plaintiffs' knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiffs seek to hold the Defendant responsible for the injuries the Defendant inflicted on Plaintiffs and thousands of similarly situated persons ("Class Members") due to the Defendant's impermissibly inadequate data security, which caused the personal information of Plaintiffs and those similarly situated to be exfiltrated by unauthorized access by cybercriminals (the "Data Breach") on or about November 27, 2022.

2. Defendant Gunster operates a law firm headquartered in West Palm Beach, Florida, with 12 additional offices throughout the state.[1]

3. The Data Breach initially affected 9,550 individuals.[2] The data which the Defendant collected from the Plaintiffs and Class Members, and which was exfiltrated by cybercriminals from the Defendant, were highly sensitive. The exfiltrated data included personal identifying information ("PII") and personal health information ("PHI" and, together with Personal Information, "Personal Information") such as: name, date of birth, Social Security number, and brokerage and banking information.

4. Upon information and belief, prior to and through the date of the Data Breach, the Defendant obtained Plaintiffs' and Class Members' Personal Information and then maintained that sensitive data in a negligent and/or reckless manner. As evidenced by the Data Breach, the Defendant inadequately maintained its network, platform, software—rendering these easy prey for cybercriminals.

5. Upon information and belief, the risk of the Data Breach was known to the Defendant. Thus, the Defendant was on notice that its inadequate data security created a heightened risk of exfiltration, compromise, and theft.

6. Then, after the Data Breach, Defendant failed to provide timely notice to the affected Plaintiffs and Class Members for nearly 18 months —thereby exacerbating their injuries. Ultimately, Defendant deprived Plaintiffs and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, Defendant impermissibly left

[1]Gunster, "About Us" https://gunster.com/about/about-us/ (last visited on April 29, 2024).
[2] The Topeka-Capital Journal, "Health Care Data Breaches: Gunster, Yoakley & Stewart, PA (March 8, 2024)" https://data.cjonline.com/health-care-data-breaches/gunster-yoakley-stewart-pa-fl-9550-20240308-hacking-network/ (last accessed April 29, 2024)

Plaintiffs and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

7. Even when Defendant finally notified Plaintiffs and Class Members of their Personal Information exfiltration, Defendant failed to adequately describe the Data Breach and its effects.

8. Today, the identities of Plaintiffs and Class Members are in jeopardy—all because of Defendant's negligence. Plaintiffs and Class Members now suffer from a present and continuing risk of fraud and identity theft and must now constantly monitor their financial accounts.

9. Armed with the PII stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

10. Plaintiffs and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

11. Plaintiffs and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their Personal Information, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

12. Through this action, Plaintiffs seek to remedy these injuries on behalf of themselves and all similarly situated individuals whose Personal Information was exfiltrated and compromised in the Data Breach.

13. Plaintiffs seek remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

14. Plaintiff Whalen is a natural person and resident and citizen of New York. Whalen is a former client of Defendant Gunster as beneficiary of several trusts set up and maintained by Gunster. On or about April 19, 2024, Whalen received a letter informing her of the Data Breach ("Data Breach Notification"), as described more fully below.

15. The Trust is the result of Gunster making Plaintiff Whalen the Trustee of the Trust. In so doing, huge amounts of PII, including detailed financial information, were provided to Defendant, which was then maintained in a negligent and/or reckless manner.

16. Plaintiff Rona is a natural person and resident and citizen of New York. Rona was employed as a nurse by Gunster, for several years, to provide healthcare services to Gunster's high net worth clients. Her employment concluded prior to the Data Breach. However, on or about April 19, 2024, Rona received a letter informing her that her information was compromised in the Data Breach.

17. Defendant Gunster is a Florida law firm with its headquarters and principal place of business located in West Palm Beach, Florida.[3] Gunster's clients range from startups to mid-

[3]Gunster, "About Us", https://gunster.com/about/about-us/ (last visited on April 29, 2024).

market businesses, Fortune 100 companies and international corporations, as well as individuals and families.[4]

JURISDICTION AND VENUE

18. This Court has original subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because both Plaintiffs (and many members of the class) are citizens of states different than that of Defendant Gunster.

19. This Court has personal jurisdiction over Defendant Gunster, because Gunster maintains its principal place of business in this district.

20. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Gunster maintains its principal place of business in the jurisdiction.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the Personal Information of Plaintiffs and Class Members

21. Defendant operates a law firm, providing legal services to individual and businesses located throughout the United States.

22. Upon information and belief, Defendant received and maintained the Personal Information of its clients and employees, such as individuals' names, dates of birth, Social Security numbers and banking and financial information, including records of wires from financial

[4] Gunster, "Practice Areas", https://gunster.com/practice-areas/ (last accessed on May 1, 2024).

institutions used to pay Defendant's fees. These records were, and continue to be, stored on Defendant's computer systems.

23. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, Defendant knew or reasonably should have known that it stored protected Personal Information and must comply with industry standards related to data security and all federal and state laws protecting customers' Personal Information and provide adequate notice to customers if their Personal Information is disclosed without proper authorization.

24. When Defendant collects this sensitive information, it promises to use reasonable measures to safeguard the Personal Information from theft and misuse.

25. Defendant acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiffs' and Class Members' Personal Information.

26. Defendant as a law firm has a fiduciary duty to Plaintiff Whalen and Client Subclass Members (as defined below).

27. By obtaining, collecting, receiving, and/or storing Plaintiffs' and Class Members' Personal Information, Defendant assumed legal and equitable duties and knew, or should have known, that they were thereafter responsible for protecting Plaintiffs' and Class Members' Personal Information from unauthorized disclosure.

28. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Personal Information, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

29. Upon information and belief, Plaintiffs and Class Members relied on Defendant to keep their Personal Information confidential and securely maintained, to use this information

for business and healthcare purposes only, to delete it in a timely fashion, and to make only authorized disclosures of this information.

30. Defendant could have prevented or mitigated the effects of the Data Breach by better securing its network, properly encrypting its data, or better selecting its information technology partners.

31. Defendant's negligence in safeguarding Plaintiffs' and Class Members' Personal Information was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

32. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiffs' and Class Members' Personal Information from being compromised.

33. Defendant failed to properly select its information security partners.

34. Defendant failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

35. Defendant failed to ensure the proper monitoring and logging of file access and modifications.

36. Defendant failed to ensure the proper training its and its technology partners' employees as to cybersecurity best practices.

37. Defendant failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the Personal Information of Plaintiffs and Class Members.

38. Defendant failed to timely and accurately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

39. Defendant knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured Personal Information.

40. Defendant failed to provide adequate supervision and oversight of the Personal Information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Personal Information of Plaintiffs and Class Members, misuse the Personal Information and potentially disclose it to others without consent.

41. Upon information and belief, Defendant failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

42. Upon information and belief, Defendant failed to ensure the proper encryption of Plaintiffs' and Class Members' Personal Information and monitor user behavior and activity to identify possible threats.

43. Further, in acting in a fiduciary capacity to its clients, Gunster held itself to the highest standards of care for its clients property, including PII.

The Data Breach

44. On or about April 19, 2024, Defendant mailed the Data Breach Notification letter (in the form attached hereto as Exhibit "A") to its former and current clients and employees, containing, among other the following statements:

> Gunster, Yoakley, & Stewart, PA ("Gunster") is a law firm that obtained your information in connection with the provision of legal services. You may not have heard of Gunster, but we provide professional legal services to clients in a wide variety of industries and business sectors. In order to serve our clients, we receive relevant data from our clients, opposing parties and third parties. We are writing to notify you of a data security incident that occurred at Gunster and involved some of your information. This notice

> explains the incident, measures taken to protect the information, and some steps you may consider taking in response. We regret that this incident occurred and apologize for any inconvenience.
>
> **What Happened?**
> Upon detecting the data security incident on November 27, 2022, we immediately took measures to contain the incident and securely restore our network. A thorough investigation was conducted with the assistance of firms that have helped other law firms address similar incidents. We determined from the investigation that there was unauthorized access to our document management file system over the weeks leading up to our discovery of the incident. After we identified the files involved, we began a process to review those files to identify the content. We also notified federal law enforcement and have been in communication with them regarding the incident.

45. The letter explained what data was stolen in the Data Breach:

> **What Information Was Involved?**
> We began reviewing the files involved, and based on that review, began providing notifications to individuals in April 2023. Our review continued and, on October 15, 2023, the review process generated a preliminary list of individuals whose information was contained in the files. We then worked to review the list and supplement it with addresses and other information to be able to identify individuals to notify. Our review confirmed that the files contained your name, date of birth, Social Security number, and medical or health insurance information.

46. It is likely the Data Breach was targeted at the Defendant due to its status as a large law firm that collects, creates, and maintains Personal Information, as well as creating and maintaining entities for wealthy clients.

47. Defendant was untimely and unreasonably delayed in providing notice of the Data Breach to Plaintiffs and Class Members.

48. Time is of the essence when highly sensitive Personal Information is subject to unauthorized access and/or acquisition. In this case, Defendant apparently waited *almost 18 months* between the discovery of the Data Breach and the notification of the Plaintiffs and Class Members.

49. The disclosed, accessed, and/or acquired Personal Information of Plaintiffs and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Personal Information to criminals. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Personal Information onto the Dark Web. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

50. Defendant charged Plaintiffs and Class Members professional fees for services that, *inter alia*, protect client assets and identities.

51. In the Data Breach Notification, Defendant made the following offer "We have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, SI Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration." This offer, made by Defendant, is woefully inadequate given that risks of identity theft do not expire within one year, and continue for a lifetime.

52. In sum, Defendant largely put the burden on Plaintiffs and Class Members to take measures to protect themselves.

53. Defendant did not provide any additional details about the attack.

54. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[5]

[5] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-

55. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[6] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[7] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

56. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

57. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' Personal Information with the intent of engaging in misuse of the Personal Information, including marketing and selling Plaintiffs' and Class Members' Personal Information.

58. Aside from the offer of 12 months of credit monitoring services, which is inadequate for reasons described above, Defendant has offered no measures to protect Plaintiffs and Class Members from the lifetime risks they each now face. As another element of damages,

---

wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed April 25, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, *https://www.bls.gov/news.release/pdf/wkyeng.pdf* (last accessed April 25, 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).

[6] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed April 25, 2024).

[7] *Id.*

Plaintiffs and Class Members seek a sum of money sufficient to provide Plaintiffs and Class Members identity theft protection services for 10 years.

59. Defendant had and continue to have obligations created by reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' Personal Information confidential and to protect such Personal Information from unauthorized access.

60. Plaintiffs and the Class Members remain, even today, in the dark regarding the scope of the data breach, what particular data was stolen, beyond several categories listed in the letter as "included" in the Data Breach, and what steps are being taken, if any, to secure their Personal Information and financial information going forward. Plaintiffs and Class Members are left to speculate as to the full impact of the Data Breach and how exactly the Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

61. Plaintiffs' and Class Members' Personal Information and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Personal Information and financial information for targeted marketing without the approval of Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the Personal Information and/or financial information of Plaintiffs and Class Members.

Defendant Failed to Comply with FTC Guidelines

62. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[8] To that end, the FTC has issued numerous

[8] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed April 25, 2024).

guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exfiltration of Personal Information.

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[9] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

64. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

65. The FTC recommends that companies not maintain Personal Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[10]

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[9] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed April 25, 2024).

[10] *See Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 16, 2024).

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

68. Despite its alleged commitments to securing sensitive data, Defendant does not follow industry standard practices in securing Personal Information.

69. Experts studying cyber security routinely identify financial service providers as being particularly vulnerable to cyberattacks because of the value of the Personal Information which they collect and maintain.

70. Several best practices have been identified that at a minimum should be implemented by financial service providers like Defendant, including but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

71. Other best cybersecurity practices that are standard in the financial service industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

72. Defendant failed to meet the minimum standards of any of the following

frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

73. Such frameworks are the existing and applicable industry standards in the financial service industry. Defendant failed to comply with these accepted standards, thus opening the door to criminals and the Data Breach.

The Experiences and Injuries of Plaintiffs and Class Members

74. Plaintiffs and Class Members are current and former clients and employees of Gunster.

75. As a prerequisite of obtaining legal services from, or being employed by, the Defendant, the Defendant required its clients and employees —like Plaintiffs and Class Members—to disclose their Personal Information.

Plaintiff Whalen's Experience

76. Plaintiff Whalen is a former client of Defendant Gunster. Whalen was a beneficiary of several trusts set up and maintained by Gunster, one of which is the Trust.

77. Gunster made Plaintiff Whalen the Trustee of the Trust which controlled all of Plaintiff Whalen's financial assets. In so doing, large amounts of PII, including detailed financial

information, were provided to Defendant, which was then maintained in a negligent and/or reckless manner.

78. On or about April 19, 2024, Whalen received the Data Breach Notification.

79. Plaintiff Whalen has since experienced significant emotional distress, while devoting considerable time to securing her accounts and monitoring for additional fraudulent activity.

80. To mitigate the risks associated with her PII being misused, Plaintiff Whalen has placed security freezes on her credit reports and activated fraud alerts. These alerts ensure that her identity is verified before any credit is extended to ensure that there is no fraud.

81. As Trustee of her own trust and manager of her LLC and other personal accounts, Plaintiff Whalen has spent significant time and effort contacting the Secretary of State to ensure no new certificates are filed on her name or her company's name. She has also spent more than five hours to confirm that no unauthorized fraudulent activity has taken place on her Tax ID numbers, using her compromised credentials.

82. Plaintiff Whalen has also experienced a high volume of phishing emails and text messages since the Data Breach, including fraudulent emails and text messages with misleading claims of unauthorized transactions and links to malicious websites causing her ongoing fear and anxiety regarding her PII being misused.

83. In seeking to address the harm caused by the Data Incident, Plaintiff Whalen retained the undersigned counsel to pursue legal remedies and prevent further misuse of her PII.

Plaintiff Rona's Experience

84. Plaintiff Rona was employed as a nurse by Defendant to provide healthcare services to its high net worth clients. As part of her employment, Plaintiff Rona provided Gunster with

her PII, including but not limited to her bank account number, Social Security Number and driver's license.

85. Rona's employment by Gunster concluded prior to the Data Breach. However, on or about April 19, 2024, she was notified that her information was included in the Data Breach. Notably, the letter misspelled the Plaintiff's name as "Roma" and incorrectly stated that Gunster obtained Rona's information in her capacity as a client, rather than employee.

86. Rona suffered severe consequences from the Data Breach. As a result of the Data Breach, criminals repeatedly attempted to steal funds from her bank account, resulting in the filing of a police report. Further, as detailed below, as a result of the Data Breach, Rona was prevented from closing a real estate transaction. She suffered significant monetary damages as a result.

87. After the Data Breach occurred, but before she was notified of the Data Breach, Rona attempted to exchange a property in Boca Raton, Florida, for a property in New York City, pursuant to IRS Code §1031. What should have been a routine transaction was derailed by the Data Breach, resulting in financial loss to Rona.

88. Unbeknownst to Rona, her PII had been stolen in the Data Breach, and criminals were using it to steal her money. Specifically, on or about August 30, 2023, a thief attended at Rona's bank branch in Queens, New York, with a replica of her Florida drivers' license and withdrew $5,000. The next day, the thief attempted to withdraw a further $60,000 but was prevented from doing so by bank personnel, who then alerted Rona. Rona filed a police report for grand larceny in respect of these criminal acts, but the suspect was never apprehended.

89. As a result of the Data Breach, Rona had to lock and freeze her bank accounts. She locked her Equifax credit report and alerted Social Security Administration and Florida DMV. These steps required a considerable amount of time and effort, to be particularized at trial.

90. Further, the co-op board of the New York property Rona was planning to acquire as part of the IRS Code §1031 transaction denied her purchase, because it could not access her financial information to approve the transaction, due to the security measures undertaken as a result of the Data Breach.

91. Plaintiff Rona lost the opportunity to acquire the New York property and had to pay $23,000 in capital gains taxes in respect of the Florida property disposition, as a direct result of the Data Breach.

Injuries Inflicted Upon All Plaintiffs and Class Members

92. When Defendant finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's Breach Notice fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Data Breach was perpetrated by, and the extent to which those data elements were compromised.

93. Because of the Data Breach, Defendant inflicted injuries upon Plaintiffs and Class Members. And yet, Defendant has done little to provide Plaintiffs and the Class Members with relief for the damages they suffered.

94. All Class Members were injured when Defendant caused their Personal Information to be exfiltrated by cybercriminals.

95. Plaintiffs and Class Members entrusted their Personal Information to Defendant. Thus, Plaintiffs had the reasonable expectation and understanding that Defendant would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents.

Plaintiffs and Class Members would not have entrusted their Personal Information to Defendant had they known that Defendant would not take reasonable steps to safeguard their information.

96. Plaintiffs and Class Members suffered actual injury from having their Personal Information compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their Personal Information—a form of property that Defendant obtained from Plaintiffs; (b) violation of their privacy rights; (c) the likely theft of their Personal Information; (d) fraudulent activity resulting from the Data Breach; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

97. Further, the tax employer identification number ("EIN") and brokerage account numbers of Class Members' various accounts and of legal entities formed by Gunster no longer give clients the benefit of the protections they had asked Gunster to provide from the beginning of relationships.

98. As a result of the Data Breach, Plaintiffs and Class Members also suffered emotional distress because of the release of their Personal Information—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiffs and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their Personal Information for nefarious purposes like identity theft and fraud.

99. Plaintiffs and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

100. Because of the Data Breach, Plaintiffs and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiffs and the Proposed Class Face Significant Risk of Present and Continuing Identity Theft

101. Plaintiffs and Class Members suffered injury from the misuse of their Personal Information that can be directly traced to Defendant, as detailed above.

102. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's Personal Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

103. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[11]

104. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiffs and Class Members suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Personal Information is used;

b. The diminution in value of their Personal Information;

c. The compromise and continuing publication of their Personal Information;

[11]Anne Saita, "Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims", Threat Post, (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited on April 26, 2024).

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Personal Information; and

h. The continued risk to their Personal Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Personal Information in their possession.

105. Stolen Personal Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Personal Information can be worth up to $1,000.00 depending on the type of information obtained.[12]

106. The value of Plaintiffs' and the proposed Class's Personal Information on the black market is considerable. Stolen Personal Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

[12] Brian Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on April 26, 2024).

107. It can take victims years to spot or identify Personal Information theft, giving criminals plenty of time to milk that information for cash.

108. One such example of criminals using Personal Information for profit is the development of "Fullz" packages.[13]

109. Cyber-criminals can cross-reference two sources of Personal Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

110. The development of "Fullz" packages means that stolen Personal Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Personal Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including

[13] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, "Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm," KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/ (last visited on April 26, 2024).

this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen Personal Information is being misused, and that such misuse is fairly traceable to the Data Breach.

111. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

112. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and the Class that their Personal Information had been stolen.

113. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

114. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their Personal Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

115. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Personal Information. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

116. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated

that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[14]

Defendant Failed to Comply with FTC Guidelines

117. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[15] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[16]

118. According to the FTC, unauthorized Personal Information disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[17] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the "FTCA").

---

[14] "Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable," FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on April 26, 2024).

[15] "Start With Security, A Guide for Business," FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 26, 2024).

[16] *Id.*

[17] "Taking Charge, What to Do If Your Identity is Stolen," U.S. DEPARTMENT OF JUSTICE, at 3 (January 2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited on April 26, 2024).

119. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. See *In the matter of Lookout Services, Inc.*, No. C-4326, Complaint ⁋ 7 (June 15, 2011) ("[Respondent] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Respondent] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Respondent] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . .").

120. These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of Personal Information.

Defendant Failed to Comply with HIPAA

121. Because of its involvement with electronic personal health information ("PHI"), Defendant is a "Business Associate" as defined under the rules and regulations promulgated

pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (45 CFR Parts 160 to 164). The HIPAA "Security Rule," published in 2003, addresses the requirement that both Covered Entities and Business Associates, as defined therein, adopt security procedures to assure the confidentiality, integrity, and availability of personal health care information, or PHI (45 CFR Part 160 and Subparts A and C of Part 164).[18]

122. Business Associates are directly liable for violations of the HIPAA Security Rule (See HITECH Act 13401, 42 U.S.C. 17931 (making 45 CFR 164.308, 164.310, 164.312, and 164.316 directly applicable to business associates, as well as any other security provision that the HITECH Act made applicable to covered entities); 45 CFR 164.306, 164.308, 164.310, 164.312, 164.314, 164.316.

123. Data Breach is a Security Incident under HIPAA because it impaired both the integrity (data is not interpretable) and availability (data is not accessible) of PHI held by Gunster:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[19]

124. The Data Breach is also considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.402.[20]

---

[18] The Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited April 30, 2024).
[19] FACT SHEET: Ransomware and HIPAA, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last visited March 2, 2024).
[20] *Id.*

125. The Security Incident Procedures standard at 45 C.F.R. § 164.308(a)(6)(i) requires a covered entity to implement policies and procedures to address security incidents. The associated implementation specification for response and reporting at § 164.308(a)(6)(ii) requires a covered entity to identify and respond to suspected or known security incidents, mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes.

126. Defendant failed to comply with HIPAA, both prior to and after suffering the Data Breach.

127. Charged with handling highly sensitive Personal Information including, financial information, and health and medical insurance information, Defendant knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's customers as a result of a breach. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

128. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has failed to adequately protect the Personal Information of Plaintiffs and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

129. Defendant's failure to properly and promptly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their

Personal Information and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

130. Plaintiffs bring this action individually and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

131. Plaintiffs propose the following Class definition:

> All persons residing in the United States whose Personal Information was compromised, accessed, exfiltrated, or otherwise impacted by the Data Breach.

132. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

133. Excluded from the Class are: (i) Gunster, any Entity in which Gunster has a controlling interest, and individuals who at any time since November 27, 2022 served as Gunster directors or officers; (ii) any judge, justice, or judicial officer presiding over the Action and the members of their immediate families and judicial staff; and (iii) any individual who timely and validly opts out of the Settlement.

134. Plaintiffs and Class Members satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

135. **Numerosity**. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals who reside in the U.S. and were or are clients or employees of Gunster, and whose Personal Information was compromised by the Data Breach.

136. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Personal Information;

b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their Personal Information;

f. If Defendant breached its duty to Class Members to safeguard their Personal Information;

g. If Defendant failed to comply with the HIPAA Security Rule (45 CFR 160 and Subparts A and C of Part 164) by failing to implement reasonable security procedures and practices to protect the integrity and availability of PHI;

h. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. If Defendant should have discovered the Data Breach earlier;

j. If Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

k. If Defendant failed to provide notice of the Data Breach in a timely manner;

l. If Defendant's delay in informing Plaintiffs and Class Members of the Data Breach was unreasonable;

m. If Defendant's method of informing Plaintiffs and Class Members of the Data Breach was unreasonable;

n. If Defendant's conduct was negligent;

o. If Plaintiffs and Class Members were injured as a proximate cause or result of the Data Breach;

p. If Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

q. If Defendant breached implied contracts with Plaintiffs and Class Members;

r. If Defendant was unjustly enriched as a result of the Data Breach; and

s. If Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

137. **Typicality**. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach. Moreover, all Plaintiffs and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

138. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and

experienced in litigating complex class actions. Plaintiffs have no interests that conflict with, or are antagonistic to, those of the Class.

139. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs and Class Members' data was stored on the same network system and unlawfully and inadequately protected in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

140. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

141. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

142. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

143. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above, including in paragraph 136.

144. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

145. Plaintiffs re-allege and incorporate by reference paragraphs 1-144 of the Complaint as if fully set forth herein.

146. Defendant required its employees and contractors to submit Plaintiffs' and Class Members' non-public Personal Information to Defendant to receive Defendant's services.

147. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer system—and Plaintiffs' and Class Members' Personal Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes so it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

148. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable to Defendant. Given that Defendant holds vast amounts of Personal Information, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of Personal Information.

149. After all, Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiffs and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the Personal Information entrusted to them.

150. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its, or its service providers', systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

151. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that its own, and its service providers', systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

152. Defendant failed to take appropriate measures to protect the Personal Information of Plaintiffs and the Class. Defendant is morally culpable, given the prominence of security breaches in the financial services industry, including the insurance industry. Any purported safeguards that Defendant had in place were wholly inadequate.

153. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Personal Information by failing to adopt, implement,

and maintain adequate security measures to safeguard that information, despite known data breaches in the financial service industry, and allowing unauthorized access to Plaintiffs' and the other Class Members' Personal Information.

154. The Defendant was negligent in failing to comply with industry and federal regulations in respect of safeguarding and protecting Plaintiffs' and Class Members' Personal Information.

155. But for Defendant's wrongful and negligent breach of its duties to Plaintiffs and the Class, Plaintiffs' and Class Members' Personal Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the Personal Information of Plaintiffs and the Class and all resulting damages.

156. Defendant owed Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to its Personal Information. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures to protect its Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

157. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendant actively sought and obtained the Personal Information of Plaintiffs and Class Members.

158. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Personal Information;

b. Failing to comply with—and thus violating—FTCA, HIPAA and the applicable regulations;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Personal Information;

f. Failing to detect in a timely manner that Class Members' Personal Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

159. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial service industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' Personal Information would result in one or more types of injuries to Class Members.

160. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting

Plaintiffs' and the other Class Members' Personal Information. Defendant knew or should have known that its systems and technologies for processing and securing the Personal Information of Plaintiffs and the Class had security vulnerabilities.

161. As a result of Defendant's negligence, the Personal Information and other sensitive information of Plaintiffs and Class Members was compromised, placing them at a greater risk of identity theft and their Personal Information being disclosed to third parties without the consent of Plaintiffs and the Class Members.

162. Simply put, Defendant's negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their Personal Information by criminals, improper disclosure of their Personal Information, lost benefit of their bargain, lost value of their Personal Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

163. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

164. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for a period of ten years.

SECOND CAUSE OF ACTION
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

165. Plaintiffs re-allege and incorporate by reference paragraphs 1-144 of the Complaint as if fully set forth herein.

166. Under the Federal Trade Commission Act, Defendant had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data.[21]

167. Moreover, Plaintiffs' and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

168. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Personal Information.

169. Defendant violated its duties and its obligations under HIPAA as a Business Associate by reason of the Data Breach.

THIRD CAUSE OF ACTION
Implied Contract
(On Behalf of the Plaintiffs and the Class)

170. Plaintiffs re-allege and incorporate by reference paragraphs 1-144 of the Complaint as if fully set forth herein.

171. Plaintiffs and Class Members were required to deliver their Personal Information to Defendant as part of the process of obtaining financial services from Defendant.

[21] 15 U.S.C. § 45.

172. Defendant solicited, offered, and invited Class Members to provide their Personal Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Personal Information to Defendant.

173. Defendant accepted possession of Plaintiffs' and Class Members' Personal Information, for the ostensible purpose of contracting with Plaintiffs and Class Members, either as clients or as employees.

174. Plaintiffs and Class Members entrusted their Personal Information to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

175. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including FTC guidelines on data security) and were consistent with industry standards.

176. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide Personal Information, was the latter's obligation to: (a) use such Personal Information for business purposes only, (b) take reasonable steps to safeguard that Personal Information, (c) prevent unauthorized disclosures of the Personal Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Personal Information, (e) reasonably safeguard and protect the Personal Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Personal Information only under conditions that kept such information secure and confidential.

177. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

178. Plaintiffs and Class Members paid money to the Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

179. Plaintiffs and Class Members would not have entrusted their Personal Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

180. Plaintiffs and Class Members would not have entrusted their Personal Information to Defendant in the absence of its implied promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

181. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant. Defendant, on the other hand, breached its obligations under the implied contracts with Plaintiffs and Class Members by failing to safeguard their Personal Information and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

182. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Personal Information; (iii) lost or diminished value of Personal Information; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly

increased risk to their Personal Information, which (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

183. Plaintiffs and Class Members are entitled to compensatory, consequential and nominal damages suffered as a result of the Data Breach.

184. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (1) strengthen their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for a period of ten years.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff Whalen and Client Subclass Members)

185. Plaintiff Whalen and the Client Subclass Members re-allege and incorporate by reference paragraphs 1-144 of the Complaint as if fully set forth herein.

186. Defendant as a law firm has a fiduciary duty to Plaintiff Whalen and Client Subclass Members, under contract, statute and common law. Further, Gunster became a fiduciary by its undertaking to collect and maintain that Personal Information of its clients within the lawyer-client relationship.

187. As Plaintiff Whalen's and the Client Subclass Members' fiduciary, Gunster was obligated to act primarily for Plaintiff Whalen and the Client Subclass Members (a) to safeguard of Plaintiffs and Class Members' Personal Information in its custody; (b) to timely notify Plaintiff Whalen and the Client Subclass Members of a Data Breach and disclosure of their Personal Information; and (c) to maintain complete and accurate records of what information (and where) Gunster did and does store.

188. Gunster had and has a fiduciary duty to act for the benefit of Plaintiff Whalen and the Client Subclass Members upon matters within the scope of Gunster's relationship with them, which includes safeguarding their Personal Information.

189. Because of the highly sensitive nature of the Personal Information Plaintiff Whalen and the Client Subclass Members provided to Gunster, Plaintiff Whalen and the Client Subclass Members (or their third-party agents) would not have entrusted Gunster, or any other law firm in Gunster's position, to retain their Personal Information had they known the reality of Gunster's inadequate data security practices.

190. Gunster breached its fiduciary duties to Plaintiff Whalen and the Client Subclass Members by failing to sufficiently encrypt or otherwise protect Plaintiff Whalen's and the Client Subclass Members' Personal Information from unauthorized disclosure.

191. Gunster also breached its fiduciary duties to Plaintiff Whalen and the Client Subclass Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

192. As a direct and proximate result of Gunster's breaches of fiduciary duties owed to Plaintiff Whalen and the Client Subclass Members, Plaintiff Whalen's and the Client Subclass Members' sensitive Personal Information was accessed and exposed through the Data Breach.

193. Defendant further charged "fiduciary fees" to Plaintiff Whalen and the Client Subclass Members at high professional rates allegedly to protect Plaintiffs and Class Members by acting as legal fiduciaries.

194. It is clear from the outcome of the Breach that Gunster did not act to protect Plaintiff Whalen and the Client Subclass Members from harm, or act adequately as fiduciaries.

195. As a direct and proximate result of Gunster's breach of its fiduciary duties, Plaintiff Whalen and the Client Subclass Members have suffered and will continue to suffer numerous injuries and consequential damages, as detailed *supra*.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff Whalen and Client Subclass Members)

196. Plaintiff Whalen and the Client Subclass Members re-allege and incorporate by reference paragraphs 1-144 of the Complaint as if fully set forth herein.

197. This Claim is pleaded in the alternative to Third Cause of Action, above.

198. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff Whalen and the Client Subclass Members.

199. As such, a portion of the legal fee payments made by or on behalf of Plaintiff Whalen and the Client Subclass Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

200. Plaintiff Whalen and the Client Subclass Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Personal Information. In exchange, Plaintiff Whalen and the Client Subclass Members should have received from Defendant the goods and services that were the subject of the transaction and have their Personal Information protected with adequate data security.

201. Defendant knew that Plaintiff Whalen and the Client Subclass Members conferred a benefit which Defendant accepted, in the form of legal fees, a portion of which was to be spent on cybersecurity, and in the form of Plaintiffs' Personal Information which is in itself valuable to

Defendant. Defendant profited from these transactions, kept the funds that it should have used for cybersecurity, and used the Personal Information of Plaintiff Whalen and the Client Subclass Members for business purposes.

202. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff Whalen and the Client Subclass Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff Whalen and the Client Subclass Members by utilizing cheaper, ineffective security measures. Plaintiff Whalen and the Client Subclass Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

203. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff Whalen and the Client Subclass Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

204. Defendant failed to secure Plaintiff Whalen's and the Client Subclass Members' Personal Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

205. Defendant acquired and kept the Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

206. If Plaintiff Whalen and the Client Subclass Members knew that Defendant had not reasonably secured their Personal Information, they would not have agreed to provide their Personal Information to Defendant.

207. Plaintiff Whalen and the Client Subclass Members have no adequate remedy at law.

208. As a direct and proximate result of Defendant's conduct, Plaintiff Whalen and the Client Subclass Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Personal Information is used; (c) the compromise, publication, and/or theft of their Personal Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Personal Information in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff Whalen and the Client Subclass Members.

209. As a direct and proximate result of Defendant's conduct, Plaintiff Whalen and the Client Subclass Members have suffered and will continue to suffer other forms of injury and/or harm.

210. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff Whalen and the Client Subclass Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff Whalen and the Client Subclass Members overpaid for Defendant's services.

211. These amounts include transactional work Defendant performed for Plaintiff Whalen and the Client Subclass Members at high professional rates, allegedly to Plaintiff Whalen and the Client Subclass Members.

212. Defendant further charged "fiduciary fees" to Plaintiff Whalen and the Client Subclass Members at high professional rates allegedly to protect Plaintiffs and Class Members by acting as legal fiduciaries.

213. It is clear from the outcome of the Breach that Gunster did not act to protect Plaintiff Whalen and the Client Subclass Members from harm, or act adequately as fiduciaries.

SIXTH CAUSE OF ACTION
VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
(On Behalf of Plaintiff Whalen and Client Subclass Members)

214. Plaintiff Whalen and the Client Subclass Members re-allege and incorporate by reference paragraphs 1-144 of the Complaint as if fully set forth herein.

215. The FDUPTA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce hereby declared unlawful." Fla. Stat. § 501.204(1).

216. Pursuant to Fla. Stat. § 501.202, requires such claims under the FDUTPA be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

217. Plaintiff Whalen and the Client Subclass Members, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. See Fla. Stat. § 501.203(7).

218. Defendant obtained and stored the Personal of Plaintiff Whalen and the Client Subclass Members for the purpose of providing legal services to them.

219. Defendant offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. See Fla. Stat. § 501.203.

220. Defendant's offer, provision, and sale of services at issue in this case are "consumer transaction[s]" and Plaintiff Whalen's and the Client Subclass Members' Personal Information is the subject of those "consumer transactions." See Fla. Stat. § 501.212.

221. Plaintiff Whalen and the Client Subclass Members paid for or otherwise availed themselves and received services from Defendant, primarily for personal, family, or household purposes.

222. Defendant's acts and practices were done in the course of Defendant's business of offering legal services in Florida to residents of the United States.

223. The unfair, unconscionable, and unlawful acts and practices of Defendant alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

224. Defendant, headquartered in and operating and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce,

in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failing to adequately secure the Personal Information of Plaintiff Whalen and the Client Subclass Members from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about Plaintiff Whalen and the Client Subclass Members in a manner highly offensive to a reasonable person;

c. enabling the disclosure of personal and sensitive facts about Plaintiff Whalen and the Client Subclass Members without their informed, voluntary, affirmative, and clear consent;

d. failing to encrypt the Personal Information of Plaintiff Whalen and the Client Subclass Members;

e. failing to delete the Personal Information of Plaintiff Whalen and the Client Subclass Members after it was no longer necessary to retain the Personal Information;

f. storing Plaintiff Whalen's and the Client Subclass Members' Personal Information in an internet-accessible environment when such storage was unnecessary

g. continuing to accept and store Plaintiff Whalen's and the Client Subclass Members' Personal Information after it knew or should have known of the Data Breach;

h. failing to monitor and detect the movement of the Personal Information of Plaintiffs and Class Members from Defendant's network to the internet in real time;

i. purporting to still act as fiduciaries after it knew or should have known of the Data Breach;

j. failing to monitor the practices of its cybersecurity vendors; and

k. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiff Whalen and the Client Subclass Members from taking timely self-protection measures.

225. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, et seq., HIPAA and the FDUTPA, Fla. Stat. § 501.171(2).

226. Defendant knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff Whalen and the Client Subclass Members' Personal Information and that the risk of a data breach or theft was high.

PRAYER FOR RELIEF

WHEREFORE Trustee Whalen, Plaintiff Whalen and Plaintiff Rona, individually and on behalf of all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives, and the undersigned as Class Counsel;

B. An Order appointing Plaintiff Whalen as representative of the Client Subclass, and the undersigned as Class Counsel;

C. A mandatory injunction directing Defendant to adequately safeguard the Personal Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the Personal Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive

Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Personal Information;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiffs' and Class Members' Personal Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Personal Information, as well as protecting the Personal Information of Plaintiffs and Class Members;

xi. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees'

compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

D. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Personal Information to unauthorized persons;

E. A mandatory injunction requiring Defendant to purchase credit monitoring and identity theft protection services for each Class Member for ten years;

F. An injunction enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Personal Information;

G. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined, as well as transactional and fiduciary fees Gunster charged directly;

H. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

I. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

J. Granting the Plaintiffs and the Class leave to amend this Complaint to conform to the evidence produced at trial;

K. For all other Orders, findings, and determinations identified and sought in this Complaint; and

L. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

PARTIES CONSENT

Under Federal Rule of Civil Procedure 15(a)(2), a party may amend its pleadings if the opposing party consents in writing or if the court grants leave to amend. Here, the Court has granted leave to amend. Defendant herein also consents to the filing of this Second Amended Class Action Complaint.

Dated: December 23, 2024

Respectfully Submitted,

/s/ John A. Yanchunis

Brian Murray* bmurray@glancylaw.com **GLANCY, PRONGAY & MURRAY** 230 Park Avenue, Suite 358 New York, NY 10169 T: (212) 682-5340	John A. Yanchunis Florida Bar #: 324681 JYanchunis@forthepeople.com **MORGAN & MORGAN** **COMPLEX LITIGATION GROUP** 201 North Franklin Street 7th Floor Tampa, FL 33602 T: (813) 223-5505 F: (813) 223-5402

**Pro hac vice forthcoming*

Counsel for Plaintiffs and the Class